INFORMATION ON THE PROCESSING OF PERSONAL DATA – VIDEO RECORDING – UNIVERSITY LIBRARY SERVICES

Which of your data will be processed?	What purpose your data will be used for?	What is the background to processing your personal data?	How long shall we store your data?	Data controller	Data processor
video recording	For reasons of the protection of property, there are cameras working in the rooms and places open to the readers.	Justified interest: Law CXXXIII. of 2005 regarding the rules of activities related to the protection of persons, property, and the work of detective agencies 30-31. §[1]	3 working days counted from the time of recording of the data	person working as a guard of property, 1056 Budapest, Szerb u. 21-23. III. em. 316. +36 1 411-6500/3410	-

Your rights[2]:

1. right to transparent information **– You may request information relating to the processing of your personal data any time;**
2. right to access your personal data **– You may access your personal data controlled by us**
3. upon your request you have the right for rectifying and erasing („right to be forgotten") your personal data and the right to restrict the processing of your personal data **– If your personal data is processed incorrectly, please, make a note and we will correct, erase it, etc.**
4. information regarding the recipients **– You must be informed if we have forwarded your personal data to somebody;**
5. the right to data portability (only in the case of automatic data processing of personal data controlled upon consent or contract) – **If you need it, we give you your personal data;**
6. right to object **– You may object to the processing of your personal data upon legitimate interest any time;**
7. in case of automated decision-making **– The right not to belong under the scope of such decision. Please, let us know of any such incident.**
8. right to legal remedies **– In case of any infringement of your rights, you may turn to the data protection officer, the National Authority for Data Protection and the Freedom of Information or a court.**

Where to turn for legal remedy or if you have questions?

To the data protection officer of the University

Data protection officer of ELTE:
Kinga Rigó, Doctor of Law
ELTE Rector's Cabinet
Office for Handling Data and Strategic Information
H-1053 Budapest, Ferenciek tere 6.
Phone: +36 1 411-6500 /2855
E-mail: kinga.rigo@rk.elte.hu

To the National Authority for Data Protection and the Freedom of Information

National Authority for Data Protection and the Freedom of Information:
H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Website: www.naih.hu
Phone: +36-1-391-1400

To a court

In Hungary a law suit can be initiated either at a court in the native country of the data subject or at his/her dwelling place, depending on the choice of the person concerned.

[1] The text of legal regulations referred to are included in Annex 1.

[2] For the details see https://konyvtar.elte.hu/en/data-processing-agreement

Annex 1

30-31. § of the Law CXXXIII. of 2005 regarding the rules of activities related to the protection of persons, property, and the work of detective agencies

Article 30 (1) The guard may make, process and control image, sound and image and sound recordings, through the operation of the electronic observation system, within the framework of the contract defining his obligations for the fulfilment of his contractual obligations under the law of information self-determination and freedom of information, bearing in mind the restrictions imposed by this law. A person carrying out the tasks of the guard is considered a data controller.

(2) The guard may apply electronic monitoring systems exclusively to private areas or to the part of the private area used by the general public if the natural person expressly agrees to it. The consent may also be granted by conduct. In particular, it is considered consent by conduct when a natural person enters the part of a private area open to the public in spite of a statement made in accordance with Article 28 (2), unless circumstances clearly lead to another conclusion.

(3) Electronic surveillance systems must not be used where observation can offend human dignity, in particular in changing rooms, fitting rooms, washrooms, lavatories, hospital rooms, and residential parts of social institutions.

(4) The guard may record, and use data recorded by a telemonitoring system, by means of a security system protecting the data and information system within the framework of the contract defining his obligations for the fulfilment of his contractual obligations under the law of information self-determination and freedom of information, bearing in mind the restrictions imposed by this law.. The provisions of Section 31 apply to the processing and control of these data. A person carrying out the tasks of the guard is considered a data controller.

Article 31 (1) The electronic surveillance system, making the recording of images, sound or image and sound possible, may be applied to protect human life, bodily integrity, personal liberty, to guard dangerous substances, to protect business, payment, bank, and securities, and to safeguard property, if circumstances make it likely that the detection of infringements of law, the flagrance delicto of perpetrators, or the prevention of such offenses or their proving would be impossible by other means, further more the use of these technical means is indispensable, and there is no disproportionate restriction on the right to self-determination.

(2) Image, sound or image and sound recordings shall be destroyed or cancelled not later than three working days after recording if not used.

(3) In the absence of use, the recorded image, sound or image and sound shall be destructed or erased at the latest thirty days after the recording, if the recording was made

a) at a public event to protect human life, physical integrity, personal liberty,

b) to prevent acts of terrorism and public accidents at a public event, at a public transport station, at a stop (e.g. train station, airport, and metro station)

c) to ensure the safe storage, handling and transportation of money, securities, precious metals and gems of at least significant value under the Criminal Code Act

(d) to protect dangerous substances.

(4) In the absence of use, the recorded image, sound, image and sound shall be destroyed or cancelled sixty days after recording at the latest, if the purpose of the recording was the protection of private territories open to the public necessary for the performing of the duties of persons offering

(a) financial services, supplementary financial services,

b) mortgage-banking activities,

c) investment services, stock exchange activities,

d) custody of securities,

e) clearing house activity,

f) insurance, insurance intermediaries, insurance advisory services.

(5) It is deemed use in the sense of paragraphs 2 to 4 if the recorded image, sound or image and sound or other personal data is used as evidence in a court or for another official procedure.

(6) Any person whose right or legitimate interest is affected by the recording of an image, sound, or image and sound recording or other personal data may, in accordance with paragraphs 2, 3 and 4, ask the controller of the image, sound or image and sound recording, or other personal data not to destruct or erase the data within three working days, or within thirty or sixty days after having certified his right or justified interest. Upon the request of a court, a public prosecutor's office, a detective authority, an authority engaged in preparatory procedures, or other authority the recorded image, sound, image and sound recordings and other personal data will immediately be sent to the court or authority. If there is no request made for data within thirty days after the request not to destruct the data, the recorded image, sound, and image and sound recording, and other personal data must be destructed, or erased, except if the deadline in paragraph (3) or (4) has not expired yet.

(7) Only the person engaged in the protection of persons or property is entitled to see the recorded image, sound, or image and sound recordings or other personal data who would not be able to perform his duties fixed in his/her contract without it, and if getting to know the data is indispensable to the prevention or interruption of the violation of law. The name of the person engaged in the protection of persons or property, who are responsible for the recording and controlling of image, sound, or image and sound recordings, or other personal data as well as the reason and time for getting acquainted with the data must be recorded in a report.